在私有网络和公共网络之间通过预置共享、NAT 超载配置路由器间的 IPSec

目录

简介

此示例配置显示如何使用 IPSec 加密专用网络 (10.103.1.x) 和公用网络 (98.98.98.x) 之间的数据流。98.98.98.x 网络可通过专用地址识别 10.103.1.x 网络。10.103.1.x 网络可通过公用地址识别 98.98.98.x 网络。

先决条件

要求

本文档需要对 IPSec 协议拥有基本的了解。有关 IPSec 的详细信息，请参见 IP 安全 (IPSec) 加密简介。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 软件版本 12.3(5)
- Cisco 3640 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

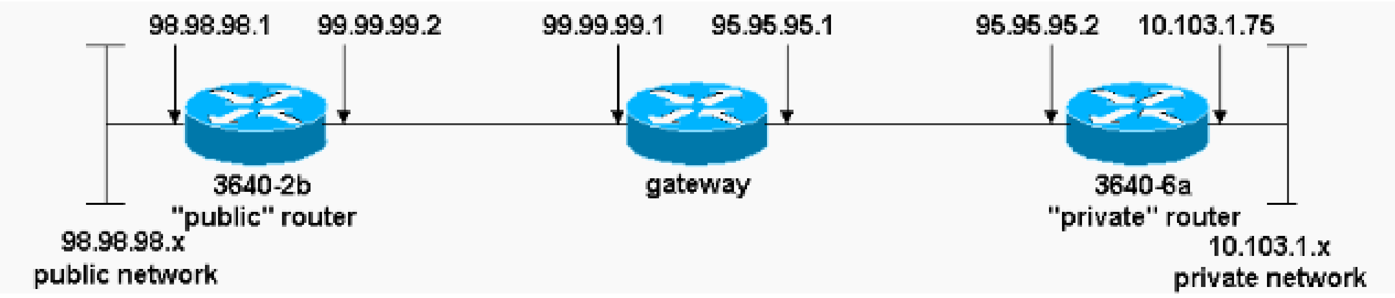
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用此图所示的网络设置。



配置

本文档使用以下配置：

- 3640-2b“公用”路由器
- 3640-6a“专用”路由器

3640-2b“公用”路由器

```
rp-3640-2b#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-2b
!
ip subnet-zero
!

!
!--- Defines the Internet Key Exchange (IKE) policies.
crypto isakmp policy 1

!--- Defines an IKE policy. Use the crypto isakmp policy
!--- command in global configuration mode. IKE policies
!--- define a set of parameters !--- that are used
```

```
during the IKE phase I negotiation.


hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 95.95.95.2

!--- Configures a preshared authentication key, used in
!--- global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an acceptable !---
combination of security protocols and algorithms, !---
which has to be matched on the peer router. ! crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to !--- establish the
IPSec security associations (SAs) that protect !--- the
traffic specified by this crypto map entry. set peer
95.95.95.2

!--- Sets the IP address of the remote end. set
transform-set rtpset

!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- This is used to assign an extended access list to a
!--- crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. ! interface Ethernet0/0 ip address
98.98.98.1 255.255.255.0 no ip directed-broadcast !
interface Ethernet0/1
ip address 99.99.99.2 255.255.255.0
no ip directed-broadcast
no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use !--- the crypto map
"rtp" for IPSec. ! . . !--- Output suppressed. . . ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.1

!--- Default route to the next hop address. no ip http
server ! access-list 115 permit ip 98.98.98.0 0.0.0.255
10.103.1.0 0.0.0.255

!--- This access-list option causes all IP traffic !---
that matches the specified conditions to be !---
protected by IPSec using the policy described by !---
the corresponding crypto map command statements.


access-list 115 deny ip 98.98.98.0 0.0.0.255 any

!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

3640-6a“专用”路由器

```

rp-3640-6a#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!

!
ip subnet-zero




!--- Defines the IKE policies. ! crypto isakmp policy 1

!--- Defines an IKE policy. !--- Use the crypto isakmp
policy !--- command in global configuration mode. IKE
policies !--- define a set of parameters !--- that are
used during the IKE phase I negotiation.


hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 99.99.99.2

!--- Configures a preshared authentication key, !---
used in global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an !--- acceptable
combination of security protocols and algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to establish !--- the
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. set peer 99.99.99.2

!--- Sets the IP address of the remote end. set
transform-set rtpset

!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- Used to assign an extended access list to a !---
crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. . . !--- Output suppressed. . . ! interface
```

```
Ethernet3/0 ip address 95.95.95.2 255.255.255.0 no ip
directed-broadcast ip nat outside

!--- Indicates that the interface is !--- connected to
the outside network. no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use the !--- crypto map
"rtp" for IPSec. ! interface Ethernet3/2 ip address
10.103.1.75 255.255.255.0 no ip directed-broadcast ip
nat inside

!--- Indicates that the interface is connected to !---
the inside network (the network subject to NAT
translation). ! ip nat pool FE30 95.95.95.10 95.95.95.10
netmask 255.255.255.0

!--- Used to define a pool of IP addresses for !--- NAT.
Use the ip nat pool command in !--- global configuration
mode.


ip nat inside source route-map nonat pool FE30 overload

!--- Used to enable NAT of !--- the inside source
address. Use the ip nat inside source !--- command in
global configuration mode. !--- The 'overload' option
enables the router to use one global !--- address for
many local addresses.


ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1

!--- Default route to the next hop address. no ip http
server ! access-list 110 deny ip 10.103.1.0 0.0.0.255
98.98.98.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any

!--- Addresses that match this ACL are NATed while !---
they access the Internet. They are not NATed !--- if
they access the 98.98.98.0 network. access-list 115
permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255

!--- This access-list option causes all IP traffic that
!--- matches the specified conditions to be !---
protected by IPSec using the policy described !--- by
the corresponding crypto map command statements.


access-list 115 deny ip 10.103.1.0 0.0.0.255 any

route-map nonat permit 10
match ip address 110
!

!
line con 0


line vty 0 4
```

```
!
end
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

要验证此配置，请尝试源来自专用路由器 10.103.1.75 上以太网接口的扩展 ping 命令，该命令会发送至公用路由器 98.98.98.1 上的以太网接口。

- ping - 用于诊断基本网络连接。

  ```
  rp-3640-6a#ping
  Protocol [ip]:
  Target IP address: 98.98.98.1
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
  Extended commands [n]: y
  Source address or interface: 10.103.1.75
  Type of service [0]:
  Set DF bit in IP header? [no]:
  Validate reply data? [no]:
  Data pattern [0xABCD]:
  Loose, Strict, Record, Timestamp, Verbose[none]:
  Sweep range of sizes [n]:
  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 98.98.98.1, timeout is 2 seconds:
  !!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
  ```
- show crypto ipsec sa - 显示当前 (IPsec) SA 所采用的设置。
- show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。
- show crypto engine - 显示加密引擎的配置信息汇总。请在特权 EXEC 模式下使用 **show crypto engine 命令。**

show 输出示例

此输出是在中心路由器上发出的 **show crypto ipsec sa 命令的输出。**

```
rp-3640-6a#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 95.95.95.2

   protected vrf:
   local  ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0)
   current_peer: 99.99.99.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
     path mtu 1500, media mtu 1500
     current outbound spi: 75B6D4D7

     inbound esp sas:
      spi: 0x71E709E8(1910966760)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4576308/3300)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x75B6D4D7(1974916311)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4576310/3300)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

此命令用于显示对等体之间构建的 IPSec SA。加密隧道在95.95.95.2和99.99.99.2之间建立，用于网络98.98.98.0和10.103.1.0之间的流量。您可以看到两个封装安全负载(ESP)SA已建立和出站。由于没有 AH，因此，未使用认证报头 (AH) SA。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

注意：在发出debug命令之前，请参阅有关Debug命令的重要信息。

- **debug crypto ipsec sa - 用于查看第 2 阶段的 IPSec 协商。**
- **debug crypto isakmp sa - 用于查看第 1 阶段的 ISAKMP 协商。**
- **debug crypto engine - 用于显示加密会话。**

相关信息

- NAT 运行顺序
- IP安全故障排除-了解和使用debug命令

- IPSec 支持页面
- NAT 支持页
- 技术支持 - Cisco Systems